Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK OPONENTA BAKALÁŘSKÉ PRÁCE

Jméno studenta: Jan Nedbal

Název práce: Analýza a návrh nasazení SIEM řešení v prostředí středního podniku

Autor posudku: Ing. Ondřej Hornig

Cíl práce: Cílem práce je provést podrobnou analýzu požadavků a dostupných řešení SIEM s přihlédnutím k požadavkům zákona o kybernetické bezpečnosti. Autor práce podrobně zmapuje požadavky vycházející ze zákona o kybernetické bezpečnosti, norem ISO a navrhne jeho plnění s využitím SIEM. V praktické části autor vypracuje případovou studii, zohledňující aktuální požadavky na monitoring bezpečnosti s využitím vhodného SIEM řešení.

Povinná kritéria hodnocení práce	**Stupeň hodnocení** (známka)			
	A	**C**	**E**	**F**
Práce svým zaměřením odpovídá studovanému oboru	☒	☒	☐	☐
Vymezení cíle a jeho naplnění	☐	☒	☒	☐
Zpracování teoretických aspektů tématu	☒	☐	☐	☐
Zpracování praktických aspektů tématu	☐	☐	☒	☐
Adekvátnost použitých metod, způsob jejich použití	☐	☒	☐	☐
Hloubka a správnost provedené analýzy	☐	☒	☒	☐
Práce s literaturou	☐	☐	☒	☐
Logická stavba a členění práce	☐	☐	☒	☐
Jazyková a terminologická úroveň	☐	☒	☐	☐
Formální úprava a náležitosti práce	☐	☒	☒	☐
Vlastní přínos studenta	☐	☒	☒	☐
Využitelnost výsledků práce v teorii (v praxi)	☐	☒	☒	☐

Dílčí připomínky a náměty:

Autorovi se při exportu práce vytratila čísla stránek.
Ve 2.4 (a možná i jinde) autor nesprávně využívá různého řádkování a umístění citací. Autor také střídá různé řezy písma (kap. 4.1). Tabulky autorovi přetékají mimo okraje stránky (nejen kap. 4.2). Čtenář se tak může lehce ztratit.

Dle mého názoru nejde zaměňovat pojmy ISO 27000 za ISO 27k.
Použité obrázky nejsou v práci vloženy v dostatečné kvalitě.
Kapitola 4.4 popisující konkrétní vybrané řešení je převzata (pouze přeložena) z http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.6/com.ibm.qradar.doc/c_hwg_app_overview_m3.html. Zdroj je uveden pouze v seznamu. Stejně tak https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.6/com.ibm.qradar.doc/shc_qradar_comps.html.
Autor neseřadil zdroje ani podle jednoho přípustného kritéria, vyhledávání v nich je velmi ztíženo.

Celkové posouzení práce a zdůvodnění výsledné známky:

Práce se skládá ze 7 kapitol, první kapitola představuje úvod práce, ve druhé kapitole autor pojednává o ISO standardech zabývajících se zkoumanou problematikou, ve třetí kapitole autor rozebírá platnou českou legislativu, zvláště ve vztahu k Zákonu o kybernetické bezpečnosti. V kapitole 4 je představen SIEM jako pojen a základní produkt. Případová studie s kalkulací přínosů a nákladů pro typové organizace je ukázána v kapitole 5. Šestá kapitola čtenáři předkládá shrnutí výsledků, na které navazuje závěr práce v kapitole 7.
Formální a stylistická úprava práce většinově odpovídá platným metodickým pokynům pro vypracování závěrečné práce. Práce je relativně čtivá, i když v některých místech (například kapitola 2.4) by bylo vhodné použít další strukturaci práce pomocí podkapitol. Zároveň práce obsahuje velké množství marketingových formulací a částí textu, které by v akademické práci mohly být opomenuty. Autor pracoval převážně s aktuálními zdroji, které bohužel v některých místech textu chybí. Práce představuje ve své teoretické části kvalitní souhrn vytyčené problematiky.
Cíle práce vytyčené při jejím zadání byly částečně naplněny, postrádám pouze akademický nadhled nad technologiemi a případné (alespoň lehké) srovnání s dalšími aplikacemi (které je i součástí cílů práce vytyčených při jejím zadání), výrobci a přístupy. Praktická část práce připomíná spíše případovou studii pro konkrétní prodejní případ.

Otázky k obhajobě:

Jste schopen najít jiné řešení SIEM? Popište jeho parametry ve srovnání s IBM. Zároveň představte i nějaké open-source řešení.
Můžete přiblížit možnosti využití kompatibilního hardware, jak zmiňujete pod obrázkem 20?

Práci doporučuji k obhajobě.

Navržená výsledná známka: E - dobře

V Hradci Králové, dne 23. května 2016

_____

podpis